インターネットを利用した犯行予告
ウイルス供用事件の検証結果

平成２４年１２月

大阪府警察

目　次

はじめに　・・・・・・・・・・・・・・・・・・１
１　事案概要　・・・・・・・・・・・・・・・・・１
２　捜査経過　・・・・・・・・・・・・・・・・・２
(1)　事件の認知及び捜査体制の確立
(2)　接続機器を特定するための捜査
(3)　Ａ氏の嫌疑性に関する捜査
(4)　その他の捜査
３　強制捜査の着手　・・・・・・・・・・・・・・６
(1)　Ａ氏の嫌疑性の検討
(2)　逮捕の必要性の検討
４　起訴に至るまでの捜査　・・・・・・・・・・・７
(1)　捜査状況
(2)　Ａ氏の犯人性について
(3)　起訴
５　Ａ氏の釈放に至る経緯と遠隔操作ウイルス「iesys.exe」に関する捜査　・・８
６　捜査指揮上の問題点　・・・・・・・・・・・・９
７　解析作業における問題点　・・・・・・・・・・９
８　取調べにおける問題点　・・・・・・・・・・１０
９　再発防止対策　・・・・・・・・・・・・・・１０
(1)　証拠の総合的な評価と被疑者供述吟味の徹底
(2)　人的・物的基盤（ツール等）の強化
(3)　部門間の連携強化と早期捜査体制の確立
(4)　広域的･専門的捜査の推進
(5)　有識者等との連携強化
おわりに　・・・・・・・・・・・・・・・・・１１

平成２４年１２月
大 阪 府 警 察

インターネットを利用した犯行予告･ウイルス供用事件の検証結果

はじめに

本年７月２９日、大阪市が管理するホームページに、無差別大量殺人を予告する書き込みがなされ、ＩＰアドレス※1に対する捜査等を基に無実の市民を真犯人と誤って逮捕するという極めて遺憾な事案が発生した。

大阪府警察において、本件捜査の問題点について検証したところであるが、以下の反省・教訓事項が認められたことから、これを真摯に受け止め、再発防止に向けた所要の取組を推進していくこととしたい。

※1　ＩＰアドレス
企業内ネットワーク、インターネット等のネットワーク上で相互に接続されているコンピュータ等を識別するために、そのコンピュータ個別に割り振られる番号。

１　事案概要

平成２４年７月３０日、大阪市職員より、大阪府南警察署に対して、市が管理するインターネットホームページの相談窓口「市民の声」に、『無差別殺人予告』が書き込まれた旨の通報があり、本事案を認知した。

認知後、掲示板に書き込まれたＩＰアドレス等の捜査からＡ氏を割り出し、８月１日、Ａ氏に任意同行を求め、パソコン等の任意提出を受けるとともに事情聴取を行った。翌２日には、Ａ氏宅に対する捜索差押えを行い、Ａ氏が使用していたパソコンの解析等の所要の捜査を実施した結果、８月２５日に逮捕状を請求、翌２６日、Ａ氏を威力業務妨害罪で逮捕した。

Ａ氏は、当初から一貫して関与を否定していたが、９月１４日大阪地方検察庁は、Ａ氏を偽計業務妨害罪で起訴した。

９月１９日、三重県警察との情報交換により、Ａ氏が使用していたパソコンから遠隔操作が可能なファイル（ウイルス）が発見されたことから、検察庁との協議の後、９月２１日にＡ氏は釈放された。

さらに捜査を進め、Ａ氏のパソコン内から発見されたファイル（ウイルス）の機能や真犯人を名乗る者からの犯行声明文の内容を精査した結果、Ａ氏は犯人ではないと判断し、大阪地方検察庁は１０月１９日、Ａ氏の起訴を取り消した。

２　捜査経過

(1)　事件の認知及び捜査体制の確立

ア　平成２４年７月３０日、大阪府南警察署（以下「南警察署」という。）に対する、「市のホームページ内に設けられた「市民の声」という相談窓口に無差別殺人予告が書き込まれた」との大阪市職員からの通報により本件を認知し、下記の書き込み内容（抜粋）から、インターネットを介した威力業務妨害事件と判断した。

【名前】　●●　●●※２

※２　「●●　●●」には、Ａ氏の漢字氏名及び振り仮名が書き込まれていた。
ただし、振り仮名は、実際のＡ氏の名の読みとは異なる。

【予告】　来週の日曜日（８／５）ヲタロードで大量殺人する

【内容】　午後２時頃歩行者天国にトラックで突っ込んで無差別にキモヲタどもを轢きまくります。
あと、ナイフで無差別に刺します。その後自殺します
かならず実行します。みなさんさようなら。

イ　南警察署は、主管所属である大阪府警察本部刑事部捜査第一課（以下「捜査第一課」という。）及び大阪府警察本部生活安全部生活安全総務課サイバー犯罪対策室（以下「サイバー対策室」という。）の支援を得て、同日から犯行予告場所を管轄する大阪府浪速警察署（以下「浪速警察署」という。）との間で、南警察署長指揮による合同捜査を開始した。

(2)　接続機器を特定するための捜査

ア　捜査の結果、本件書き込み時のＩＰアドレスが判明するとともに、本件書き込みはＡ氏のモバイルルーターから行われたこと、また、モバイルルーター自体はパソコン等をインターネットに接続する機器であるが、複数のパソコン等を同時にインターネットに接続することができる機能等を有することが判明した。

イ　前記アのルーターの接続機能の特性から、Ａ氏からの事情聴取が不可欠であると判断、８月１日、東京都練馬区内にいたＡ氏と接触し、警視庁荻窪警察署で事情聴取したところ、本件への関与を否定する一方、所持していたノートパソコン、ルーター等を任意提出したので確認したところ、ルーター等の設定は契約者情報どおりの状態であり、ルーター等の他人への貸与事実等も否定したので、本件書き込みはＡ氏のルーターに接続した機器から行われたと判断された。

ウ　さらに捜査の結果、本件書き込みと同時間帯に、Ａ氏のルーターに接続した機器から大阪市のホームページに対して、３件（本件書き込み分を含む）のアクセス事実があることが判明、同アクセス状況から犯人は、大阪市のトップページにアクセスした後、「市民の声」ページへ移動（アクセス）して本件書き込みを行い、送信したと認められた※３。

※３　大阪市のホームページには、「トップページ」や「市民の声」ページ等、複数のページがある。

エ　ルーターへの接続機器を特定するため、Ａ氏から提出を受けていたノートパソコンの解析を実施することとし、解析に先立ち、当府警に装備されたウイルス対策ソフトによるウイルスチェックを実施したが、ウイルスは検知されなかった。

オ　パソコン等からインターネットを通じてウェブサイト等へアクセスした場合、１つのアクセスに対して複数の履歴が残るのが通常であるが、Ａ氏のパソコン内には、大阪市のホームページへアクセスした際の履歴の一部しか残っておらず、意図的に履歴を消去（一部消去漏れ）したものと思われた。

カ　次に、パソコンの起動状況、ルーターの通信状況、書き込み時間の整合性を解析したところ、矛盾はなく、トップページへのアクセスから書き込み終了まで、本件書き込みを行うのに十分な時間があったことが確認された。

キ　以上捜査の結果、Ａ氏はルーターにパソコンを接続し、大阪市のホームページへアクセスして本件書き込みを行い、その後アクセス履歴を消去（一部消去漏れ）したと推定した。

(3)　Ａ氏の嫌疑性に関する捜査

ア　任意取調べ

８月１日以降、８月２６日の逮捕に至るまでの間、ポリグラフ検査を含め８回の任意取調べを実施したが、Ａ氏は本件への関与を否定し続けた。

イ　Ａ氏による犯行可能性の検討

(ｱ)　犯行当日の行動についてＡ氏から聴取し、裏付け捜査を実施したところ、本件書き込み時間帯にＡ氏は自宅内に居り、パソコンをルーターに接続して通信していたと認められた。

(ｲ)　他方、ルーターへの接続（無線ＬＡＮ※4）可能距離が最大、半径約１００メートルであることが判明したので、第三者による犯行の可能性は否定できないものの、Ａ氏が自宅内からルーターに接続したノートパソコンを使って本件書き込みを行ったとしても矛盾がないことが確認された。

※４　無線ＬＡＮ
無線でデータ通信を行う構内網のこと。
「アクセスポイント」と呼ばれる中継機器を中心として、無線通信機能を有するコンピュータ等が相互接続されてネットワークが形成される。無線 LAN に接続されたコンピュータがインターネットに接続する際にはアクセスポイントを経由する。もし、アクセスポイントの設定に不備がある場合は、悪意のある者が設定の不備を悪用してインターネットに接続することが可能となる。

ウ　第三者による犯行可能性の検討

Ａ氏は取調べに対し、第三者犯行説を主張していたことや前記イ－(ｲ)の観点から、想定される次の５つのケース

①　「Ａ氏のルーターを無断使用（無線ＬＡＮ）し、第三者が別の機器で書き込んだ」ケース

②　「Ａ氏のパソコンを使用して、直接書き込んだ」ケース

③　「「ＣＳＲＦ攻撃※5」で書き込んだ」ケース

※５　ＣＳＲＦ攻撃
クロスサイトリクエストフォージェリ（Cross site request forgeries）の略で、インターネット上のウェブサイトに対する攻撃手法の一つ。「地雷」とも呼ばれている。
悪意のある者が、この攻撃手法を悪用し、不正操作が仕組まれたウェブページを第三者に閲覧させることによって、第三者が意図せず別のウェブページに対して何らかの操作を行わせることが可能となる。

④　「遠隔操作で書き込んだ」ケース

⑤　「Ａ氏のパソコン内に潜んでいた時限設定のウイルスが自動実行し、設定された時間に書き込んだ」ケース

について検討した。

その結果、

- ①については、Ａ氏のパソコン内にアクセス履歴が残存していること
- ②については、犯行時間帯にＡ氏が在宅していたこと
- ③については、犯行予告書き込みにＡ氏の氏名の一部が用いられていること（注：メールに仕掛けられた場合を除き、ＣＳＲＦ攻撃の被利用者選定は偶然性に支配され、予め用意してある 文面中の氏名と、実際の被利用者の氏名を一致させることは極めて困難である。）
- ④については、犯行時間帯にＩＰアドレスの割り当て直しがされており、外部からのリアルタイムな遠隔捜査を継続させることが困難であること
- また、⑤も含め、ウイルス対策ソフト及び自動実行ファイルの確認結果等によれば、事前侵入したウイルスによる遠隔操作及び自動実行による犯行の可能性は窺えなかったこと

などから、第三者犯行の可能性は低いと判断された。

(4)　その他の捜査

ア　本名による書き込みについての捜査

真犯人が本名で書き込みを行う例は稀であり、疑問点として浮上したが、既述のとおり書き込みに係る履歴が消去された形跡があり、一部が消去漏れと認められたことから、犯人は履歴を消去し完全に証拠隠滅したと考えていると推測された。また、この種事件の犯人は愉快犯、自己の能力の誇示、警察に対する挑戦といった動機等から犯行を行う例が見られることから､他の捜査結果等を踏まえると、特に不自然ではないと判断した。

イ　起動確認の実施

解析の最終作業として、

① パソコンの内部構成を、押収した時点の状態のまま起動させ、動作しているプログラム等を確認する

② システムの自動バックアップ機能を利用して、パソコンの内部構成を、本件犯行時点に近い８月１日午前５時頃の状態に戻して起動させ、同様に動作しているプログラム等を確認する

という作業を行ったが、いずれの場合も不正なプログラムの動作は確認されなかった。

3　強制捜査の着手

これまでの捜査結果等を踏まえ、A氏の嫌疑性や逮捕の必要性について下記のとおり検討して、大阪地方検察庁とも協議のうえ強制捜査に着手することを決定し、８月２６日、A氏を通常逮捕するとともに関係先の捜索差押えを実施した。

(1)　A氏の嫌疑性の検討

これまでの捜査により

ア　本件書き込みは、ＩＰアドレスに基づく捜査、ルーターに関する捜査、大阪市サーバの保存記録の捜査、ノートパソコン内の履歴の解析、A氏の行動に関する供述等から、A氏が自宅において、ノートパソコンをルーターに接続した上、インターネット回線を通じて大阪市のホームページへアクセスして書き込んだと判断して、何ら矛盾がないこと。

イ　A氏主張の第三者犯行説について想定される５つのケースを検討したが、第三者犯行は困難と認められたこと。

ウ　ウイルス等については、A氏のパソコンには最新のウイルス対策ソフトが導入され正常に機能していたが、ウイルスが検知されておらず、また、押収後の解析において当府警装備の最新ウイルス対策ソフトによるスキャンでもウイルスが検知されなかったことから、パソコン内にウイルスは蔵置されていなかったと認められること。

エ　ウイルス対策ソフトでも検知されない未知のウイルスの存在を想定し、自動実行ファイルの確認を行ったが、不審点が発見されなかったこと。

オ　パソコン内に本件書き込みに係る履歴の一部が残っていることから、A氏による書き込みと判断されること。

カ　本件への関与を否定しているA氏のパソコン内より、本件書き込みに係る履歴の一部が削除されている事実と、A氏の供述が矛盾することから、証拠隠滅を図ったと認められること。

キ　A氏の供述や主張に基づき各種裏付け捜査を実施したが、関与を否定する事実が発見されなかったこと。

などから、本件はA氏による犯行と判断した。

(2)　逮捕の必要性の検討

８月１日から継続的にA氏の取調べを行うなどして、任意捜査を実施してきた

が、

ア　本件書き込みに係る履歴の消去は確認されているが、Ａ氏が関与を否定しているため消去に使用したソフトが未解明であり、また、消去の方法等も不明であること。

イ　Ａ氏は本件への関与を完全否定しており、本件書き込みの手段･方法が未解明であること。

などから、これらの点を任意捜査で追及、解明を図ろうとすれば、罪証隠滅されるおそれがあり、また、単身居住であるため、捜査の進展状況によっては逃走を図るおそれも考えられたことから、事件の全容を解明するためには、Ａ氏を逮捕した上で取調べる必要があると判断した。

4　起訴に至るまでの捜査

(1)　捜査状況

ア　供述状況

Ａ氏は弁解録取時、逮捕留置中、勾留中を通じて、任意取調べ時同様、本件への関与を否定し続けた。

イ　携帯電話の通話状況

Ａ氏の携帯電話の通話状況等から、共犯者の存在は否定された。

ウ　パソコン内の履歴の追加捜査

既述のとおり、解析の結果、アクセス時の履歴が消去（一部消去漏れあり）されていたが、通常の状態でパソコンを起動したところ、本件犯行に関する履歴は表示されなかったことから消去漏れという疑いが更に濃厚となった。

エ　ウイルス感染に関する追加捜査

既述のとおりウイルスの蔵置（感染）については否定したが、逮捕後の捜索差押え分等も含め、ＵＳＢメモリー、パソコン等を押収していたので、全てについてファイルの確認やウイルス対策ソフト（複数のソフトにより実施）によるチェックを行ったが、ウイルスや不正なプログラムは検知されなかった。

オ　ＣＳＲＦ攻撃に関する追加捜査

(ｱ)　Ａ氏宛てに地雷（添付ファイル）を仕込んだメールを送付したケースを想定して、パソコン内のメールデータをすべて確認したが、不審なファイルは

存在しなかった。

(ｲ)　大阪市サーバの保存記録にあっては、通常の書き込みの場合とＣＳＲＦ攻撃による書き込みの場合とでは異なる通信記録が残ることが確認され、追加捜査したところ、本件書き込みは通常の場合の通信記録であったことが確認された。

カ　復元実験の実施

(ｱ)　パソコン内から既に消去されているソフト等を確認するため、８月１日午前５時及び午後５時の時点の状態を復元し、確認した各ファイル(プログラム)一つ一つについて実行等してみたが、不正なプログラム特有の挙動は確認されず、ウイルスも検知されなかった。

(ｲ)　この解析中、午前５時の時点の状態の中に「iesys.exe」を含む多数のファイルが存在したので、複数のウイルス対策ソフト製品で確認したが、不正なプログラム(ファイル)は検知されなかった。

(2)　Ａ氏の犯人性について

Ａ氏から、本件犯行を認める供述は得られなかったものの、これまでの接続機器等の解析結果や裏付け捜査結果などから、Ａ氏を本件書き込みの犯人として矛盾はなく、また、Ａ氏以外には本件書き込みをなし得ないと判断した。

(3)　起訴

以上の捜査結果等を踏まえ、Ａ氏は９月１４日、大阪地方検察庁より、偽計業務妨害罪で起訴された。

５　Ａ氏の釈放に至る経緯と遠隔操作ウイルス「iesys.exe」に関する捜査

(1)　起訴から４日後の９月１８日、伊勢神宮等に対する犯行予告事件で男性を逮捕していた三重県警察から捜査協力の依頼があり、翌１９日、本件捜査に従事した当府警サイバー対策室員が三重県警察を訪問し、逮捕男性のハードディスク等を起動したところ、起動中にエラー画面が表示される等、不審な状況を確認した。

(2)　当該エラー画面を確認すると、「iesys.exe」という名称のファイルが自動実行していることを確認したが、同ファイルは、本件（大阪事件）捜査過程で、８月１日午前５時時点の状態のパソコン内に存在した「iesys.exe」と同じファイル名であったことから、同日付で三重県警察から警察庁情報通信局情報技術解析課(以

下「警察庁情報技術解析課」という。）に対し、解析の口頭依頼がなされた。

(3)　帰阪後、Ａ氏のパソコンを再確認したところ、「iesys.exe」という名称のファイルが存在することが再確認され、詳細に解析したところ、「iesys.exe」と関連するファイル内に外部の掲示板への接続を指示していると思われるURLの記載があり、三重県警察押収に係るパソコンを起動した際に同ファイルが自動実行していたことを考え合わせると、遠隔操作ウイルスである可能性が浮上した。

(4)　９月２０日、三重県警察との情報交換により、三重県警察において警察庁情報技術解析課から、「iesys.exe」は外部のサーバ等へ接続するおそれがある旨の連絡を受けたことが判明し、当府警察においても、「iesye.exe」が遠隔操作ウイルスの可能性があると判断、大阪地方検察庁へ通報し、Ａ氏は翌２１日、釈放された。

6　捜査指揮上の問題点

Ａ氏の供述の掘り下げが十分でなかった。

(1)　Ａ氏は、本件への関与は否認するものの、具体的な反論内容ではなかった（本件に関与していないので、反論が具体的でなかったのは当然のことである。）。一方、Ａ氏の供述と相反する本件関与への客観的証拠はパソコンの解析結果から得たものであり、犯人性の立証の大きな柱としたことからＡ氏の供述に対する掘り下げが十分に行われたとは言えず、供述の吟味が足りなかった。

(2)　収集した客観的証拠から犯人と判断したが、この種の高度なネットワーク犯罪においては、犯罪の手段･方法が日々変化･複雑化している現状から、犯人性認定における当該客観的証拠の意味・内容を一層慎重に検討した上で捜査を進めるべきであった。

7　解析作業における問題点

(1)　不正プログラムを発見する最も確実な方法は、コンピュータ内に存在する全てのファイル（復元可能な削除ファイルを含む。以下同じ）を解析することであるが、そのためにはより高度な技術力のほか、長期に亘る解析期間が必要となり、一都道府県警察レベルにおいては実質的に困難であった。

(2)　全てのファイルを解析することが困難であったことから、解析能力を有する捜

査員が専従して、A氏が自らインストールしたソフトウェアなど解析対象範囲を絞りこんだ解析を行ったが、不正プログラムを発見することができなかった。

(3)　本事案は、サイバー犯罪対策部門において不正プログラム等の発見、解析を実施していたが、より多角的な解析の実施について、解析能力を有する近畿管区警察局大阪府情報通信部や情報管理課と緊密に連携して組織全体としての取組を考慮すべきであった。

なお、サイバー犯罪対策部門としては、解析能力を有する捜査員を複数投入して、より多角的に解析することも検討したが、解析資機材の数量不足のため実施に至らなかった。

8　取調べにおける問題点

A氏に対する取調べについて、犯人と決め付けられ利益誘導されるなどして自白を強要された旨の報道がなされたことから、取調べに問題がなかったか否かについて調査した。

取調べ官から聴取したところ、「いずれの取調べにおいても、取調べを始める際には供述拒否権を告知した。」、「客観的証拠による立証に重点を置き、淡々と取調べを行った。」、「客観的証拠については申し向けたが、自白を強要したり利益誘導したような事実はない。」とのことであり、その他の調査結果からも不適正な取調べは確認できなかった。

9　再発防止対策

(1)　証拠の総合的な評価と被疑者供述吟味の徹底

捜査指揮官は、取調べ官の心証のみに囚われることなく、証拠を総合的に評価して、客観的証拠と供述内容の具体的な分析を実施し、否認している場合には特に弁解内容をよく聴取し第三者による犯行可能性の有無について、捜査及び検討を徹底する。

また、被疑者が自認している場合でも、客観的事実との整合性等その信用性を十分吟味検討する。

(2)　人的・物的基盤（ツール等）の強化

ア　遠隔操作を含む不正ソフトウェア、ウイルスに関する捜査員等の知識と捜査

技能が、ネットワーク関連犯罪の実情に追いついていないことを踏まえ、専門的知識・技能を有する職員の採用、育成を推進する。

さらに、現場捜査員等に対する教養・研修の一層の充実を図るとともに、この種事件捜査に当たっては部門間の横断的な捜査体制を構築し、多角的な捜査を実施していく。

イ　現場配備されているウイルス対策ソフトが１種類のみであることを踏まえ、複数の対策ソフト及び解析資機材の導入を今後検討する。

(3)　部門間の連携強化と早期捜査体制の確立

本事案において、無線ＬＡＮへの不正アクセスの可能性等については、近畿管区警察局大阪府情報通信部等から助言を受けて実施したものの、結果としてウイルスの発見に至らなかったことを踏まえ、捜査の初期段階からパソコンの解析依頼を検討する等、担当部門間の恒常的な連携を保持し、詳細な情報の共有を図り、的確な捜査体制を確立する。

(4)　広域的･専門的捜査の推進

この種犯罪は、捜査手法が確立していないことに加えて、ネットワークを利用し全国レベルで発生することから、広域的･専門的捜査が不可欠である。

よって、警察庁、全国警察での広域的･専門的捜査を推進するため、不正プログラム検体使用の疑いが生じた段階での警察庁への報告を徹底し、組織的対応を図る。

(5)　有識者等との連携強化

ネットワーク関連犯罪の捜査にあっては、日々高度化･グローバル化が進展していることを鑑み、最新のソフトウェア、ウイルス等の情報が必要であることから、専門的知識･技術を持った有識者、研究機関等との連携が不可欠である。

その実効性を担保するために、警察庁不正プログラム解析センターに加え、ウイルス対策等を専門とする研究機関等からの情報提供･共有を可能とする仕組みを検討し、捜査支援体制の強化に資する。

おわりに

本件事案では、ＩＰアドレス等の客観証拠の精査を捜査の柱とし、Ａ氏のアリバイ捜査を行う等、捜査を進めたが、高度なネットワーク犯罪に対する捜査力が十分では

なく、結果として犯人ではないＡ氏を逮捕するという遺憾な事態に至ってしまった。

ネットワーク関連犯罪については、今後、この種犯罪に対応する組織、関係部門との協力体制を一層強化し、高度な知識を有する捜査員の育成が急務であるとともに、巧妙、高度化する同種犯罪には、全国的な組織的対応、支援ができる仕組みが不可欠であると痛感した。

大阪府警察においては、本事案を教訓とし、事件ごとの特性を踏まえた捜査方針の樹立及び事件指揮並びに証拠と犯人との結び付き等、あらゆる可能性を考慮して、慎重を期した捜査を徹底するとともに、本検証に当たって得られた再発防止対策を推進して、二度と同じ過ちを繰り返さぬよう緻密な捜査を展開して、事案の真相を解明するという警察の使命を果たすための不断の努力をもって、警察捜査に対する信頼回復を図っていく所存である。

以　上